

The Potential Gain section needs modification.

The potential gain is not every ballot. Only the ballots whose positions were switched and where one of the switched positions were voted would be affected. Unless the attack was more of an attention grabbing type attack intended to be obvious, the gain may not even be effective. It is at this point that the author introduced the issue of the type of implementation because method used can have a big impact on the potential gain.

1. Pure switch. The candidate whose gain is desired (Cand A) is switched with a candidate who is expected to make a better showing (Cand B). The difference may be very small because most of the vote changes will cancel each other out. The difference will be the spread between the higher vote count and the lower vote count (typically, the absolute $|Cand\ B - Cand\ A| < Cand\ A$). If the initial assumption that Cand B will be higher than Cand A is false, the change will result in a loss. Note that the change does not even need to be made in every precinct, especially if there are different positions due to rotation or placement in different precincts. (In many systems, a particular candidate's position can change between ballots due to rotation rules, trying to place the maximum number of candidates on one ballot, or just plain error. This can be particularly difficult to catch in ballot proofing because a Cand A position may be correct in, for an example, 9 out of 10 ballots and displaced in the 10th.)
2. Minor candidate add. A lesser candidate who is expected to get a few votes (Cand A and Cand B are both greater than Cand C) position is redefined to be the same as Cand A. Then $Cand\ A = Cand\ A + Cand\ C$ and $Cand\ C = 0$ where A and C is the final count result. But in this case the gain is only Cand C (Cand B - Cand A). This will tend to be subtle but may be so subtle it is ineffective (when $Cand\ B > Cand\ A + Cand\ C$). It is vulnerable to detection, especially when it is applied widely enough to effect every precinct because Cand C will have no votes in every case it is applied and observers are more likely to know and be able to prove that at least $X > 0$ votes should have occurred..

Dr Jones claims that the likelihood of detection is slight if carefully done. This assertion is true only if good Logic and Accuracy (L&A) test procedures are not performed and/or physical security of the election program installation is weak. His paper does well in highlighting some common bad practices and issues in this regard. Unfortunately many voting jurisdictions are guilty of those bad practices and some are even encouraged in this by the vendors for other reasons. Best practices with the L&A and basic physical security of the election program installed will also be effective in many other threats to the ballot definition integrity and most ballot logic attacks that are not based on a time bomb or a swap out of control code after the L&A is completed.

This is a good example of a problem that is more likely to occur as an election programming error than a deliberate attack, especially where local procedures are so poor as to not detect it in L&A. Its more serious effect is that it can give a very graphic appearance of deliberate subversion of the election when it is only human error or incompetence.

Steven V. Freeman